IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(Alexandria Division)

Ana Rodriguez, individually and on behalf of all others similarly situated, Plaintiff, v. Stratford University, Inc., Defendant.	**Case No.:** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Ana Rodriguez ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Stratford University, Inc. ("Stratford University" or "Stratford" or "Defendant").

NATURE OF THE ACTION

1. This is a class action for damages with respect to Stratford University, Inc. for its failure to exercise reasonable care in securing and safeguarding its students' sensitive personal data, collectively known as Personally Identifiable Information ("PII" or "Private Information").

2. This class action is brought on behalf of students at Stratfor University whose sensitive PII was stolen by cybercriminals in a cyber-attack that accessed student information through on Stratford University's systems on or around April 6, 2022 (the "Data Breach").

3. Stratford University reported to Plaintiff that information compromised in the Data Breach included her PII.

4. As a result of the Data Breach, Plaintiff and other Class members have experienced or will experience various types of misuse of their PII in the coming years, including but not limited to: unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial accounts.

5. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and other members of the class—defined below. These failures put Plaintiff and other Class members' Private Information at a serious, immediate, and ongoing risk. Additionally, Defendant's failures caused costs and expenses associated with the time spent and the loss of productivity from taking time to address and attempt to ameliorate the release of personal data, as well as emotional grief associated with constant monitoring of personal banking and credit accounts. Mitigating and dealing with the actual and future consequences of the Data Breach has also created a number of future consequences for Plaintiff and Class members—including, as appropriate, reviewing records of fraudulent charges for services billed

but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their personal information, and the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach.

6. Plaintiff and Class members suffered a loss of the property value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of the loss of the property value of personal information in data breach cases.

7. There has been no assurance offered from Stratford University that all personal data or copies of data have been recovered or destroyed.

8. Accordingly, Plaintiff asserts claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, violations of the Virginia Consumer Protection Act, Va. Code Ann. § 59.1-196, *et seq.*, as well as a claim for declaratory relief.

PARTIES, JURISDICTION, AND VENUE

A. Plaintiff Ana Rodriguez

9. Plaintiff Ana Rodriguez is a citizen of Woodbridge, Virginia, and brings this action in her individual capacity and on behalf of all others similarly

situated.

10. Ms. Rodriguez has been a student at Stratford University since 2019. To receive academic services at Stratford, Plaintiff Rodriguez was required to disclose her PII, which was then entered into Stratford's database and maintained by Defendant. In maintaining her information, Defendant expressly and impliedly promised to safeguard Plaintiff Rodriguez's PII. Defendant, however, did not take proper care of Ms. Rodriguez's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In April of 2022, Plaintiff Rodriguez received an email notification from Defendant stating that her sensitive PII was taken.

11. The notification was and continues to be ineffective for Rodriguez and other Class members. For example, Stratford utterly failed to describe which information was involved incident, who gained access to that information, or when that information was released to cybercriminals. Plaintiff and Class members now face an increased risk of identity theft due not only to the Data Breach itself, but also because of Stratford University's failure to

12. Some of the damages that will occur with respect to absent Class members have already manifested themselves in Plaintiff Rodriguez's experience. On July 21, 2022, Ms. Rodriguez received a notification through her McAfee ID Theft Protection software that her Social Security number had been found on the

Dark Web, a known data trafficking website that cybercriminals use to exchange information to perpetrate identity theft. It is therefore unquestionable that Plaintiff Rodriguez has suffered damaged related to the Data Breach.

13. In the months and years following the Data Breach, Ms. Rodriguez and the other Class members will continue to experience a slew of harms as a direct result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, applications for financial services requested in students' names without their permission, and targeted advertising without student consent.

14. Plaintiff Rodriguez greatly values her privacy, especially in her educational information, and would not have paid the amount that she did for Stratford University's services if she had known that her information would be maintained using inadequate data security systems.

B. Defendant Stratford University

15. Defendant Stratford University, Inc., a Virginia corporation, is a private university based in Virginia. Its principal place of business is located in Alexandria, Virginia at 2900 Eisenhower Avenue, Floor 2, Alexandria, Virginia 22314. Stratford University offers a number of undergraduate and graduate programs to students through campuses in Virginia, Maryland, and India. Stratford's data storage policies and practices, are established in, and emanate from, the state of Virginia.

C. Jurisdiction

16. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

17. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

D. Venue

18. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the class's claims also occurred in this District.

FACTS

19. Defendant is a private, for-profit university that offers a number of graduate and undergraduate programs to students within a variety of disciplines. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable laws.

20. In April of 2022, Defendant first learned of an unauthorized entry into its network, which contained students' Private Information. Defendant sent the

following message to students in an email through the university's Corporate Communications account:

> Dear valued student,
>
> At Stratford University, we value transparency and respect the privacy of your information, which is why we are writing to let you know about a data security incident that may involve your personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.
>
> On April 6, 2022, we learned that we were the victim of a cyber-attack. Once we found out, we quickly took steps to secure and safely restore our systems and operations. Further, we immediately engaged third-party forensic and incident response experts to assist in the remediation efforts and to conduct a thorough investigation into the nature and scope of the incident. We also contacted the FBI to inform them of the incident and to seek guidance. Our investigation is ongoing, but, as of now, we have no evidence indicating any of your information has been used for identity theft or financial fraud.
>
> We appreciate your patience and understanding as we work to resolve this matter. We intend to keep you and the rest of the community updated when we learn more information. However, if you have questions, please contact us by emailing Compliance@stratford.edu. Thank you again.
>
> Sincerely,
>
> Dr. Richard Shurtz, President.

21. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected students\, which

resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

22. Stratford's notice of the Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, what information was accessed, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many students were affected by the Data Breach.

23. Given the nature of the Data Breach, Plaintiff and Class members' PII is—and for months has been—for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff and Class members' unencrypted, unredacted information, including but not limited to names, dates of birth, Social Security numbers, and financial information.

24. The Breach occurred because Defendant failed to take reasonable measures to protect the PII it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

25. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through unauthorized access by an unknown third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

26. Stratford University made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

27. In its Notice of Privacy Practices, Defendant stated the following:

> **Use of Your Personal Data**
>
> The Company may use Personal Data for the following purposes:
>
> To provide and maintain our Service, including to monitor the usage of our Service.
>
> To manage Your Account: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.

For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.

To contact You: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.

To provide You with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.

To manage Your requests: To attend and manage Your requests to Us.

For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.

For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

> With Service Providers: We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You.
>
> For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
>
> With Affiliates: We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
>
> With business partners: We may share Your information with Our business partners to offer You certain products, services or promotions.
>
> With other users: when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside. If You interact with other users or register through a Third-Party Social Media Service, Your contacts on the Third-Party Social Media Service may see Your name, profile, pictures and description of Your activity. Similarly, other users will be able to view descriptions of Your activity, communicate with You and view Your profile.
>
> With Your consent: We may disclose Your personal information for any other purpose with Your consent.

28. Stratford University describes how it may use and disclose information for each category of uses or disclosures, none of which provide it a right to expose

students' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

29. By failing to protect Plaintiff and Class members' Private Information, and by allowing the Data Breach to occur, Stratford University broke these promises to Plaintiff and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Students' Private Information

30. Stratford acquires, collects, and stores a massive amount of its students' protected PII, including personally identifiable private information.

31. As a condition of engaging in student services, Stratford University requires that these students entrust them with highly confidential Private Information.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class members' Private Information, Stratford assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class members' Private Information from disclosure.

33. Defendant had obligations created by industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

35. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

36. Before, during, and after the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

37. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant was aware that companies who store sensitive Private Information have been frequent targets of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

38. In fact, Defendant has been on notice for years that companies who store sensitive Private Information are a prime target for scammers because of the amount of confidential customer information maintained.

39. Defendant was also on notice that data breaches have been on the rise at educational institutions. The FBI has repeatedly warned companies within the education industry that hackers were targeting them. In March of 2021, for example, the FBI's Cyber Division issued a warning stating that unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors

use [ransomware] to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments."[1]

40. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[2] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[3] That trend continues.

41. Data Breaches related to educational institutions continued to rapidly increase into 2022 when Stratford University was breached.[4]

42. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[5]

43. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

---

[1] Federal Bureau of Investigation—Cyber Division, *Increase in PYSA Ransomware Targeting Education Institutions*, (Mar. 16, 2021), https://www.ic3.gov/Media/News/2021/210316.pdf

[2] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[3] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[4] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[5] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

44. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[6]

45. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities

[6] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[7]

46. These are basic, common-sense email security measures. Stratford University, with its heightened standard of care, should be doing even more. By taking these commercially reasonable, common-sense steps, Stratford University could have prevented this Data Breach from occurring.

47. Charged with handling sensitive PII including Social Security numbers, Stratford University knew, or should have known, the importance of safeguarding its students' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Stratford University Students as a result of a breach. Stratford University failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

[7] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

48. The PII was also maintained on Stratford's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. The potential for cyberattacks and the resultant improper disclosure of Plaintiff and Class members' PII was a known risk to Stratford, and thus Stratford was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

49. The fact that Plaintiff and Class members' Private Information was stolen—and is being trafficked on the Dark Web—demonstrates the monetary value of the Private Information.

50. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiff and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

51. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and financial fraud.[8] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive

[8] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

information on multiple underground Internet websites, commonly referred to as the dark web.

52. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

53. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[10]

54. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for

[9] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[10] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

analysis—and profit.[11]

55. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[12] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

56. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[13]

57. The value of Plaintiff and Class members' Private Information on the black market is substantial. Sensitive consumer information can sell for hundreds of

[11] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.
[12] *Web's Hot New Commodity*, *supra* note 17.
[13] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

dollars. It can be used to create fake insurance claims, take out loans in a person's name, or request government services that an individual is unaware of.

58. The ramifications of Stratford's failure to keep its students' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

59. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[14] This gives thieves ample time to perpetrate multiple fraudulent purchases under the victim's name.

60. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the educational institutions.

61. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the cyberattack into their systems and, ultimately, the theft of their students' Private Information.

[14] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

62. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[15] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[16] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

63. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[15] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[16] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

64. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiff and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

65. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. Stratford University's Conduct violated FTC Standards

66. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for

[17] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

businesses.[18] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

68. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[18] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[19] *Start with Security*, *supra* note 32.

70. Stratford University was at all times fully aware of its obligation to protect the Private Information of students because of its position as an educational institution. Stratford University was also aware of the significant repercussions that would result from its failure to do so.

E. Damages to Plaintiff and the Class

71. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

72. The ramifications of Stratford University's failure to keep students' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[20]

73. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

[20] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

74. Defendant further owed and breached its duty to Plaintiff and Class members to notify past and present students affected by the data breach in a timely manner.

75. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff and Class members' Private Information as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

76. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

77. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiff's case. Ms. Rodriguez received a cryptically written notice email from Defendant stating that her information was released, with no other explanation of where this information could have gone, or who might have access to it.

78. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, services billed in their name, and similar identity theft.

79. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

80. Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with Stratford University. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

81. Plaintiff and Class members would not have given their information to Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

82. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

83. The theft of Social Security Numbers is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[21] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[22] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[23]

84. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[24]

85. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false

[21] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
[22] *Id.*
[23] *Id.*
[24] *Id.*

information to police during an arrest. Private Information can also be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Private Information, and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

86. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

87. The Private Information belonging to Plaintiff and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiff or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and the Class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

88. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff and Class members' Private Information from unauthorized access, use, and disclosure, as required by various

state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

89. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect student data.

90. Defendant did not properly train their employees to identify and avoid cyberattacks.

91. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and Class members' Private Information.

92. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

93. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[25]

94. Defendant's failure to adequately protect Plaintiff and Class members' Private Information has resulted in Plaintiff and Class members having to undertake credit monitoring investigations into their own finances, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Stratford's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

95. To mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

96. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is *acquired* by criminals and when it is *used* by them. Furthermore, identity monitoring programs only alert someone to the

[25] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[26]

97. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and Class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

98. The Private Information stolen in the Data Breach can be misused on its own, or it can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen

[26] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the target might agree to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

99. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data

Breach for the remainder of the lives of Plaintiff and Class members; and

- Anxiety and distress resulting fear of misuse of their Private Information.

100. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action individually and on behalf of the following nationwide class pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(2), and/or 23(b)(3). Specifically, the nationwide class consists of the following:

> **Nationwide Class:**
> All persons whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.

102. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiff seeks to represent the following state subclasses with respect to Counts One, Two, Three, and Four in the event that the Court declines to certify the Nationwide Class above, as well as with respect to her other state law claims, including their state consumer protection claims, regardless of certification of the Nationwide Class above:

Plaintiff Rodriguez seeks to represent the following state subclass with respect to Counts One, Two, Three, and Four only in the event that the Court declines to

certify the Nationwide Class above, as well as with respect to the Virginia state law claims regardless of certification of the Nationwide Class:

> **Virginia Subclass:**
> All persons in Virginia whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.

103. The Nationwide Class and the Virginia Subclass are referred to herein as the "Class." Plaintiff reserves the right to modify, change, or expand the definitions of the class based upon discovery and further investigation.

104. Excluded from the class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

105. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

106. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

107. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff and the Class's Private Information;

- Whether Defendant was negligent in failing to timely notify Plaintiff and the class of the Data breach;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the other members of the class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

108. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of themselves and other members of the class. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

109. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

110. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict with the interests of the class she seeks to represent, she has

retained counsel competent and experienced in complex class action litigation, and will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

111. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the class, making injunctive and/or declaratory relief appropriate with respect to the class under Fed. Civ. P. 23 (b)(2).

112. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the class to individually seek redress for Defendant's wrongful conduct. Even if members of the class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiff and All Class Members)

113. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

114. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as such.

115. Defendant owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

116. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

117. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information, and to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse. This permitted a malicious third party to gather Plaintiff and Class members' Private Information, as well as misuse the Private Information and intentionally disclose it to others without consent.

118. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches involving educational institutions.

119. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff and Class members' Private Information.

120. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

121. Because Defendant knew that a breach of its systems would damage thousands of its students, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

122. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its students, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

123. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

124. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

125. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing

to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

126. Through Defendant's acts and omissions described in this Complaint, Defendant breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

127. Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

128. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

129. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

130. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and All Class Members)

131. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

132. Plaintiff and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide services and, impliedly, if not explicitly, agreed to protect Plaintiff and Class members' Private Information.

133. These contracts include the privacy notices mentioned above.

134. To the extent Defendant's obligation to protect Plaintiff and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff and other Class members' Private Information, including in accordance with federal, state and

local laws; and industry standards. Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiff and other Class members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

135. A meeting of the minds occurred, as Plaintiff and other Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

136. The protection of Plaintiff and Class members' Private Information were material aspects of Plaintiff and Class members' contracts with Defendant.

137. Defendant's promises and representations described above relating to industry practices, and about Defendant' purported concern about their clients' privacy rights, became terms of the contracts between Defendant and their clients, including Plaintiff and other Class members. Defendant breached these promises by failing to comply with reasonable industry practices.

138. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by Stratford and/or otherwise understood that Stratford would protect its students' Private Information if that information were provided to Stratford.

139. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant. Defendant did not.

140. As a result of Defendant's breach of these terms, Plaintiff and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

141. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members, in the Alternative to Count II)

142. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

143. Through their course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class members' Private Information.

144. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the services agreement with Defendant.

145. The valid and enforceable implied contracts to provide student services that Plaintiff and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

146. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

147. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

148. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

149. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

150. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide services to Plaintiff and Class members; and (b) protect Plaintiff and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Class members agreed to pay money for these services, and to turn over their Private Information.

151. Both the provision of student services and the protection of Plaintiff and Class members' Private Information were material aspects of these implied contracts.

152. The implied contracts for the provision of services—contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice and Data Breach notification letter.

153. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorialize and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and protect the privacy of Plaintiff and Class members Private Information.

154. Consumers value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected. Nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

155. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and/or its affiliated entities, and paid for the provided student services in exchange for, amongst other things, the protection of their Private Information.

156. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

157. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

158. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff and Class members Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff and Class members' private information as set forth above.

159. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

160. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

161. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class

members, nor any reasonable person would have purchased services from Defendant and/or its affiliated providers.

162. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

163. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

164. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

165. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

166. In providing their Private Information to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

167. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's personal information as included in the Data Breach notification email.

168. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class members for the safeguarding of Plaintiff and Class member's Private Information.

169. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of its customers.

170. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff and Class member's Private Information.

171. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff and Class members' Private Information.

172. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect

the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (vii) the diminished value of Defendant's services they received.

173. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Violation of the Virginia Consumer Protection Act
("VCPA")
Va. Code Ann. § 59.1-196, *et seq.*
(On Behalf of Plaintiff Rodriguez and the Virginia Subclass)

174. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

175. Plaintiff, Class members, and Defendant each qualify as a person engaged in a "consumer transaction" as contemplated by the VCPA, Va. Code Ann. § 59.1-198. Defendant also qualifies as a "supplier" under § 59.1-198.

176. As alleged herein in this Complaint, Defendant engaged in deceptive acts or practices in the conduct of consumer transactions in violation of VCPA, including but not limited to:

a. Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Private Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Private Information, including

duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

h. Failing to notify Plaintiff and members of the Class of the breach of their personal information, resulting in a delay of approximately seven months between the time of the breach and when Plaintiff and the Class members were notified.

177. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of students' Private Information.

178. In addition, Defendant's failure to secure consumers' PHI violated the FTCA, and therefore violated the VCPA.

179. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

180. The aforesaid conduct constitutes a violation of VCPA, Va. Code Ann. § 59.1-196, *et seq.*.

181. The Defendant's violations of VCPA have an impact of great and general importance on the public, including Virginians. Many Virginians have used Stratford's services whom have been impacted by the Data Breach. In addition,

Virginia residents have a strong interest in regulating the conduct of its corporate citizens such as Stratford, whose policies and practices described herein affected thousands across the country.

182. As a direct and proximate result of Defendant's violation of VCPA, Plaintiff and Class members are entitled to judgment under Va. Code Ann. § 59.1-196, *et seq*, including statutory damages under the VCPA, the injunction of further violations, the recovery of actual damages, and the recovery of the costs of this action (including reasonable attorney's fees).

183. In addition to statutory damages, Plaintiff and Class members are entitled to treble damages because the Data Breach represents a willful violation of the VCPA. Defendant willfully violated the VCPA by:

- Developing and representing that it would comply with the information privacy policy posted on its website that was applicable to Plaintiff and Class members' information at the time of the breach;
- Failing to enact reasonable security measures that led to the loss of such information through the Data Breach;
- And failing to notify victims of the data breach for approximately seven months after the discovery of the breach.

184. Defendant's implied and express representations that it would adequately safeguard Plaintiff and other Class members' Private Information

constitute representations as to characteristics, uses or benefits of services that such services did not actually have, in violation of Va. Code Ann. § 59.1-196, *et seq.*

185. Defendant's implied and express representations that it would adequately safeguard Plaintiff and Class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Va. Code Ann. § 59.1-196, *et seq*. These acts were also deceptive under Va. Code Ann. § 59.1-200(14).

186. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Va. Code Ann. § 59.1-196, *et seq.*

187. These violations have caused financial injury to Plaintiff and Class members and have created an unreasonable, imminent risk of future injury.

188. Accordingly, Plaintiff, on behalf of herself and the other Class members, bring this action under the VCPA to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

COUNT IX
Declaratory Relief

189. Plaintiff repeats and realleges all paragraphs as though fully set forth herein.

190. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

191. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

192. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

193. Defendant still possesses the PII of Plaintiff and the Class.

194. Defendant has made no announcement that it has changed its data storage or security practices relating to the PII.

195. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

196. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Stratford University. The risk of another such breach is real, immediate, and substantial.

197. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Stratford University, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

198. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Stratford, thus eliminating the additional injuries that would result to

Plaintiff and Class members, along with other consumers whose PII would be further compromised.

199. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Stratford owed and continues to owe a duty to implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Stratford's systems on a periodic basis, and ordering Stratford to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and

- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For declaratory relief concluding that that Stratford owed, and continues to owe, a legal duty to employ reasonable data security to secure the Private Information with which it is entrusted, specifically including information pertaining to financial records it obtains from its clients, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

D. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, treble damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

Respectfully Submitted,
Plaintiff
By Counsel

Dated: September 14, 2022

/s/
Matthew T. Sutter, Esq., VSB No. 66741
Sutter & Terpak, PLLC
7540 Little River Tnpk.
Suite A, First Floor
Annandale, VA 22003
Tel: (703) 256-1800
Fax: (703) 991-6116
Email: matt@sutterandterpak.com

and

Nicholas A. Migliaccio, Esq.*
Jason S. Rathod, Esq.*
Migliaccio & Rathod LLP
412 H Street N.E., Suite 302
Washington, D.C. 20002
Tel: (202) 470-3520
Fax: (202) 800-2730
* Pro hac vice admission to be sought